AU/ACSC/BRANDT/AY14

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

CONSTITUTIONALITY AND LEGALITY OF NSA SURVEILLANCE PROGRAM

by

Bradley L. Brandt, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of Graduation Requirements

Advisor: Mr. Lee M. Hester

Maxwell Air Force Base, Alabama

December 2013

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the United States government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United Stated government

Contents

INTRODUCTION

When the Bill of Rights was crafted by our Founding Fathers, they felt impelled to include the Fourth Amendment to protect American citizens from "unreasonable search and seizures" unless "probable cause" was justified and a warrant issued.[1] As politics, public opinion and technology evolved over the next two hundred years, the interpretation of the Fourth Amendment has also evolved and been continuously debated by Americans and all three branches of the government. Recently, the top-secret surveillance programs of the National Security Agency (NSA) has again brought the constitutional protections of the Fourth Amendment to the forefront of national debate. At the heart is the battle between protecting civil liberties while enhancing the security of the United States against foreign and domestic enemies, particularly terrorists. Fueling that battle are different perspectives of what constitutes privacy and what limitations, if any, should be placed on the government's collection capabilities. Currently, there is no amendment or law forbidding the surveillance of foreign governments, institutions or individuals. However, the constitutionality of NSA surveillance programs collecting on American citizens associated with our enemies comes into question. Despite the bad press the NSA has received lately, the surveillance programs do not violate the principles or intent of the Fourth Amendment, however, the United States government needs to introduce more transparency to quell its critics and provide peace of mind to Americans.

BACKGROUND

In order to fully understand the surveillance debate today and the contentious issues surrounding it, background knowledge on the creation and evolution of the Fourth Amendment is required. Originally, the Fourth Amendment spawned out of the American colonialists' hatred of the British writs of assistance. Writs of assistance were general search warrants used by British authorities, such as custom agents, to enter any house or other building to search for and

seize smuggled goods. In colonial America, there was no individual income tax. Instead the Crown collected revenue by taxing the trade of goods. To avoid this tax, smuggling was rife, not just in colonial America but also in England and her other colonies. To assist custom agents in battling smuggling and therefore collect revenue, Parliament authorized writs of assistance that equipped authorities with significant powers. Writs of assistance not only allowed the unimpeded search of any building at any time, but also allowed authorities to command the "assistance" of any persons from other officials and/or neighbors. Additionally, writs of assistance were valid until six months after the death of the monarch. Whereby, new writs of assistance would need to be approved by Parliament. Due to the invasive physical nature and the power writs of assistance gave British authorities, they were very unpopular.[2]

In 1760, King George II died and new writs of assistance were issued in the American colonies despite colonialists' objections. Through the 1760s, the legality of writs of assistance were continually challenged resulting in Parliament reauthorizing the use of general writs of assistance in the 1767 Townsend Duties Act. To inflame the situation, colonists learned that English judges had already ruled writs of assistance illegal in the homeland. In the end, the situation was resolved by judges refusing to issue writs of assistance to British authorities. However, the damage was done. Writs of assistance were one of many issues that precipitated the American Revolutionary War.[3]

After independence was won and the Constitution was being drafted and debated, many Founding Fathers vividly remembered the invasive nature of general writs of assistance and feared that the new United States government would resort to similar tactics to collect federal taxes.[4] Therefore, the Fourth Amendment was created and ratified in 1791 with the rest of the Bill of Rights. It states: "The right of the people to be secure in their persons, houses, papers,

and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[5] Interesting, the Bill of Rights applied only to the Federal government and not the individual States. The States were left to decide whether to include a similar Amendment in their own State Constitutions and this balance between States' power and the Federal government continued for over 160 years. However, after the Civil War and up to the Civil Rights Movement, Southern States' law enforcement agencies and courts repeatedly targeted African-Americans with warrantless search and seizures. To stop the racist State abuses, the Supreme Court ruled in *Mapp vs. Ohio (1961)* that the Bill of Rights applied to the States through the "exclusionary clause" in the 14th Amendment. Mapp was an African-American convicted by a warrantless search. Through the Court's ruling all warrantless searches conducted by States were made illegal since the Bill of Rights and all amendments in the Constitution now applied to the States.[6]

The modern meaning of the Fourth Amendment started its journey in the 1914 Supreme Court case *Weeks vs. United States*. Previously, lawyers and judges took the literal meaning of the Fourth Amendment and only applied it to a person's actual house and personal effects in the house. In *Weeks vs United States*, the Supreme Court extended the protections of the Fourth Amendment to places of business. So, in order for law authorities to search or seize business records, they had to show "probable cause" and acquire a search warrant.[7] Additionally, in the 1920 decision of *Silverstone Lumber Company vs. United States*, Justice Holmes coined the term from the "fruit of the poisonous tree." Stating that any evidence illegally seized without a proper search warrant would be inadmissible in court and could not be used for prosecution.[8]

Of particular interest to today's debate on the constitutionality of government surveillance programs begins with the Supreme Court case *Olmstead vs United States (1928).* *Olmstead vs United States* is a perfect example of the Supreme Court taking an extreme literal interpretation of the Fourth Amendment while disregarding any improvements in technology. During the Prohibition era, Olmstead was the general manager of a crime organization that made, transported and sold illegal alcohol during the Prohibition era. In order to collect enough evidence to uncover the illegal activities of the organization, federal authorities installed warrantless phone wiretaps on telephone lines leading to his home and office. In their decision, the Court ruled that the telephone wiretaps did not violate the Fourth Amendment because there was no physical invasion of Olmstead's house or office. The Court reasoned that "the Amendment itself shows that the search is to be of material things -- the person, the house, his papers or his effects."[9] Additionally, the Court also ruled that conversations were not protected because it was not specifically included in the language of the Fourth Amendment.[10]

The Supreme Court re-confirmed the *Olmstead* ruling fourteen years later in the 1942 case, *Goldman vs. United States*. Federal authorities learned that Goldman was planning to commit fraud. In order to collect evidence, they utilized a warrantless detectaphone to listen to his phone conversations from a room adjacent to his office. Again, the Supreme Court ruled that since law enforcement officers did not physically trespass into Goldman's office and because conversations are not explicitly protected by the Fourth Amendment, the federal authorities' methods were legal.[11] Compared to 21st Century definition of privacy, the *Olmstead* and *Goldman* decisions are shocking but not necessarily surprising. Technology evolved in leaps and bounds during the 20th Century. These two court cases are evidence that the Supreme Court failed to take into consideration significant improvements in surveillance technology. By not

addressing the technology, the Court's literal interpretations of the Fourth Amendment would be continually challenged in the future.

In many ways, if the *Olmstead and Goldman* cases had been upheld, there would be no debate today regarding the NSA's surveillance programs. However, with changes in public opinion and increasing abilities of technology to encroach on the privacy of American citizens without actual physical intrusions, changes were bound to happen. The first challenge came 25 years after the *Goldman* decision in *Katz vs United States (1967). Katz* was a revisit of the legality of wiretapping a telephone without a warrant. The FBI had been tracking Katz, a suspected gambler, and installed a microphone inside a telephone booth they knew he often used to conduct his business. By listening to his phone conversations, the FBI was able to confirm their suspicions and arrested him.[12] In the ensuing case, the Supreme Court conducted a 180 degree reversal and completely overruled the *Olmstead* and *Goldman* decisions and established new interpretations regarding the Fourth Amendment. First, the Court extended the protection of the Fourth Amendment to include private conversations. The significance of this interpretation is that the Fourth Amendment not only protects physical places, but also protects people's privacy.[13] Second, with the newly afforded protection added to the Fourth Amendment, the scope of the protection was narrowed in terms of a person's "reasonable [legitimate] expectation of privacy."[14] In other words, a person talking to a friend while walking down the street would not pass the test of "reasonable expectation of privacy" since anybody could overhear the conversation. However, a person in the privacy of their own home or, in this case, a phone booth, would expect their phone conversation to be private and thus protected. The Court's third interpretation of *Katz* restated the importance of the Fourth Amendment's warrant requirement. The Court stressed that all searches, with few exceptions, conducted without a warrant to show

probable cause would be considered a violation of the Fourth Amendment, and therefore the evidence inadmissible in court.[15] *Katz vs United States* was a momentous decision in the history of the Fourth Amendment and the United States, and set a strong foundation to ensure the privacy protection of Americans. *Katz also* setup future battles with the government over the proper balance of protecting privacy while also providing security against foreign and domestic enemies and is still referenced today as a litmus test for privacy.

The next significant Supreme Court decision is *United States vs United States District Court (1972).* In this case, the United States Justice Department charged three men with conspiring to destroy government property with one of the defendants having already succeeded. Federal law enforcement had obtained permission from the General Attorney authorizing wiretaps of the three men's phones without a judicial warrant. The Attorney General argued that his permission to collect intelligence by means of warrantless electronic surveillance was legal under the President's "national security exception" power in the Constitution. The "national security exception" clause gave the President power to protect the United States from any domestic threats to overthrow the government. The United States District Court ruled that the General Attorney's authorization for the wiretaps violated the Fourth Amendment's protection against warrantless search and seizures. The Supreme Court then ruled unanimously upholding the District Court's decision. The Supreme Court ruled that the President's power to protect the national security of the United States was not a carte blanche to conduct warrantless domestic surveillance on American citizens. They argued that the safeguards of the Fourth Amendment could not be properly guaranteed by the Executive Branch alone. They argued that the Judicial Branch, as a neutral party, needed to validate "probable cause" for a warrant to conduct electronic surveillance on American citizens. Furthermore, the Court ruled that it would not

have been difficult or taken a significant amount of time for federal authorities to acquire a proper search warrant and therefore the use of the "national security exception" was invalid.[16]

The importance of this Court decision was the curbing of government power to conduct warrantless electronic surveillance on American citizens. Even the persuasive argument of protecting the national security of the United States from violent overthrow by a domestic organization was overruled. In the majority opinion, Justice Powell pointedly asked, where does it stop? Are draft dodgers, Black Muslims, the Ku Klux Klan, or civil rights activists a clear and present danger to the existence of the Government?[17] Additionally important is what the Court did not address, which was the legality of conducting foreign intelligence surveillance on non-American citizens located inside or outside the United States. By not addressing the issue, law enforcement agencies were technically legal do conduct warrantless surveillance on foreigners in the interests of national security.

CONGRESSIONAL ACTS

In an unrelated coincidence, two days prior to the Supreme Court's *United States vs United States District Court* decision in June 1972, five men were arrested breaking and entering into the Democratic National Committee Headquarters in what would eventually culminate as the Watergate Scandal. While the far reaching consequences of the Watergate scandal are numerous, one particular product was the 1978 Foreign Intelligence Surveillance Act (FISA). Prior to FISA, it was common practice by the Executive Branch to exercise the Constitution's "national security exception" to the Fourth Amendment to conduct warrantless surveillance. Due to President Nixon and his administration's exposed abuses of conducting warrantless surveillance on their political rivals and other domestic organizations, Congress enacted FISA to provide judicial and congressional oversight while balancing the need for government

surveillance activities located within the United States.[18] The ultimate goal of the FISA legislation was to provide maximum flexibility between protecting national security while ensuring the rights guaranteed by the Fourth Amendment.

FISA created two federal courts of law, the Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court Review (FISCR). FISC judges are appointed by the Chief Justice of the Supreme Court and originally consisted of seven judges, but is now eleven. The FISCR is a three judge panel. FISA permits the surveillance of foreign persons located within the United States for a period of up to one year. However, if that surveillance were to exceed one year or, more importantly, branched out to include American citizens, then a FISA court order would be required to conduct surveillance on that individual. The law enforcement agency conducting the surveillance, for example the FBI, would need to demonstrate probable cause to the FISC. If approved, then the FISA court order would suffice as the search warrant to conduct physical or electronic surveillance. If the FISC were to deny the court order, then the requesting agency could appeal to the FISCR. If approved by the FISCR, then the agency could conduct their surveillance. If disapproved, the law enforcement agency would need to rework the probable cause justification or wait until further information made their justification stronger. In no case would warrantless surveillance be done on American citizens. FISA also required congressional oversight and was accomplished through periodic reports provided to Congressional Committees. However, it is important to highlight the secrecy in which the Court conducts its business. All requests submitted to FISC and FISC decisions are classified and not released to the public.

After enacted in 1978, FISA would be amended several times over the next few decades, however, the most significant and controversial amendments would occur after the World Trade

Center and Pentagon attacks on September 11, 2001. Before the 9/11 attacks, there was little national debate about government encroachment on the privacy of American citizens. While FISA seemed to balance national security with Fourth Amendment protections, it did create second order effects between law enforcement and foreign intelligence agencies. In 1976, the Church Committee that investigated the Watergate Scandal, recommended the FBI be limited to only investigating "conduct rather than ideas or associations."[19] This recommendation was codified in FISA and therefore hampered the FBI's ability to proactively prevent illegal foreign activities in the United States. Over time this created a wall between the FBI and other foreign intelligence agencies that inhibited the sharing of foreign intelligence in reference to national security. This lack of intelligence sharing and coordination between federal agencies would be highlighted in the 9/11 Report as a significant obstacle that could have potentially prevented the attacks.

The Bush administration reacted to the 9/11 attacks in several ways that resulted in multiple changes to FISA during the first decade of the 21st Century. First was the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, otherwise known as the Patriot Act. The Patriot Act was far-reaching and therefore controversial. The Act greatly expanded the United States' federal power in which surveillance could be conducted by lowering the FISA court order standards. From 1978 to 2001, FISA mandated the "primary purpose" of issuing a FISA court order was to collect foreign intelligence. The Patriot Act lowered the requirement to "significant purpose" creating three significant issues.[20] First, many challenged that the lower requirement violated the intent of the Fourth Amendment. Second, many asked what would happen if evidence gathered under a FISA court order was used in a criminal court case where the standards for a search warrant were

higher?[21] Thirdly, the lowering of the requirements for "probable cause" made it easier for the government to conduct domestic surveillance on American citizens at the expense of civil liberties. The main impetus behind the Patriot Act was to increase law enforcement agencies' abilities to thwart terrorist attacks. However, the Patriot Act tipped the balance towards national security at the expense of privacy. Many Americans did not challenge the Patriot Act due to the recent 9/11 attacks and felt that the government should have additional powers to hunt down terrorists, both abroad and in the United States.

Further encroaching on privacy, the Bush Administration secretly sanctioned the NSA to conduct warrantless wiretapping between 2001 and 2007 known as the Terrorist Surveillance Program (TSP). TSP was authorized by President Bush immediately after 9/11 to intercept communication between al 'Qaida and other known terrorists into and out of the United States. The purpose of TSP was to provide early warning to prevent another catastrophic terrorist attack.[22] Many considered the wiretapping illegal because the intercepted communication also included communications of American citizens. When made public, the Bush administration justified the warrantless domestic wiretapping using the President's "national security exception" power. However, that was ruled unconstitutional in *United States vs United States District Court (1972)* Supreme Court case. The wiretapping eventually stopped after media headlines, threatened lawsuits and public pressure forced the issue. The legality of the NSA wiretapping was eventually resolved when the Bush Administration agreed to have all wiretapping requests routed through the FISC as should have been done once in accordance with the law once the NSA realized American citizens were involved.

The battle between civil liberties and national security continued with the 2007 Protect America Act (PAA). In response to the NSA's TSP wiretapping scandal, the Bush

Administration instead attempted to codify into law greater surveillance powers for intelligence agencies. When TSP wiretaps were submitted to the FISC for warrants, different FISC judges held varying interpretations when a warrant should be approved and what constituted "probable cause." This hampered intelligence agencies' abilities to collect on foreigners outside the United States. The President and Congress moved quickly to pass the Protect American Act which specifically addressed these major issues. First, the PAA spelled out that electronic surveillance did not include surveillance of foreign individuals "reasonably believed" to be located outside the United States. Second, the PAA also stated that warrantless surveillance was authorized and legal if foreign individuals were located outside the United States. The PAA legally authorized the Attorney General and Director of National Intelligence (DNI) to conduct surveillance on foreigners located outside the United States for one year without a FISC court order.[23] By cutting bureaucratic red tape, intelligence agencies could more freely and efficiency collect intelligence on foreigners located outside the United States without having to always ask first. In one fell swoop, the PAA reset to the 1978 FISA procedures of conducting electronic surveillance on foreigners located outside of the United States. The third issue PAA addressed was placing limitations on liability for telecommunication companies who provided telephone records to the NSA without a FISC court order during the TSP timeframe. Through the President's "national security exception" power, the government secretly mandated that telecommunication companies provide their phone records that would be owned and stored by the NSA. The archived phone records could aid analysts in tracking known terrorists and finding new ones. However, companies turned over records without an approved FISC court order, and the ACLU and other organizations threatened to sue telecommunication companies since they deemed it illegal.[24] Lastly, the PAA stated that if intelligence agencies realized they were collecting on an American

citizen anywhere in the world or a foreign individual located in the United States, then a FISC court order was required to continue the collection of electronic surveillance.

One year after PAA, Congress passed the FISA Amendment Act of 2008 (FAA) and allowed the controversial PAA to expire. In principle, both the PAA and FAA are very similar. Like, the PAA, the FAA re-legislated the legality of intelligence agencies collecting on foreigners located outside of the United States. However, the FAA was more specific and used limited language to appease critics of the PAA. The FAA built on "reasonably believed" and added that intelligence agencies cannot "intentionally" target individuals located in the United States or an American citizen located outside the United States. The FAA also reiterated that the surveillance of anybody located within the United States or an American citizen located abroad will not be "intentionally" targeted unless "probable cause" is proven to FISC and a court order issued. Whereas the PAA was somewhat vague on these matters, the FAA was very clear. The FAA also addressed the issue of telecommunication companies providing phone records without a warrant. To prevent litigation against telecommunication companies for aiding the government over the past decade, the FAA upgraded the protection to immunity, instead of limitations on liability for past collaboration done without a FISC court order. While this controversial part of the FAA has its critics and will most likely be challenged in the future, it ensured telecommunication companies would continue to assist the government by providing phone records when issued a FISC court order. Lastly, in an attempt to appease critics and resolve Fourth Amendment concerns, the FAA states all searches "shall be conducted in a manner consistent with the Fourth Amendment of the Constitution of the United States."[25] Through this all-encompassing phrase, Congress hopes that the FAA can resist any Constitutional challenges because the spirit and intent of the Fourth Amendment is written into the legislation.

THIRD PARTY RULE

Many criticized the PAA and FAA for leaning too far towards protecting national security at the expense of civil liberties. Critics argue that despite the PAA and FAA procedures requiring a FISC court order, that by the nature of monitoring all communications in and out of the United States, American citizens would by default have their Fourth Amendment privacy rights violated. Additionally, many civil libertarians completely disagree with telecommunication companies providing third-party information about their customers. Critics believe that whomever a person calls and receives calls from should be protected under the Fourth Amendment right to privacy, and by the government mandating the collection of phone records is an unconstitutional "search and seizure" because "probable cause" has not been proven. However, *Smith vs Maryland (1979)* does not support that constitutional interpretation. In *Smith vs Maryland* police asked a phone company to install a pen register on Smith's telephone line. A pen register does not record the actual conversation, but only records what phone numbers were dialed. After proving that Smith was repeatedly calling and threatening a woman, they sought and received a search warrant to collect further evidence from his residence to prosecute him. In the decision, the Supreme Court ruled that the pen register did not constitute a warrantless search because Smith voluntarily provided the phone numbers to a third party when he dialed. The Court reasoned that Smith could not have any "expectation of privacy" when providing data to a third party.[26] It is by invoking this "third party rule" established in *Smith vs. Maryland* that the federal government justifies the request for telecommunication companies to provide records of all individuals within the United States. Telecommunication companies only store phone records for a short amount of time and then

purge them to store more recent records. Needing years of data, intelligence agencies archive the phone records from the telecommunication companies for several years.

While the "third party rule" may work for telephone records, Pandora's box has been opened when compared to data sent on the Internet. All functions accomplished on the Internet, whether emails, websites searched, documents downloaded, financial transactions, etc. are, according to *Smith*, done voluntarily by sending the data to a third party Internet Service Provider (ISP). Using the *Smith* rationale, it begs the question, does the Fourth Amendment protect emails and other Internet data from government surveillance just because individuals voluntarily sent them to an ISP?[27]

NSA SURVEILLANCE PROGRAMS

So what data are the NSA's surveillance programs collecting, why are they controversial and are they legally sanctioned by the Constitution and laws of the United States? Like most secret organizations, most of what the NSA actually does is classified. However, due to classified leaks by former NSA employee Edward Snowden, previously classified surveillance methods and types of data collected have been revealed. Due to the leaks, the NSA has admitted to collecting and storing what they call metadata. In basic terms, metadata are tags and skeletal information that flows through the Internet, but is not actual content. While metadata does not read emails, it can help the NSA determine contacts or accomplices by following the breadcrumbs.[28] The NSA uses two programs to collect specific metadata that is then stored and potentially analyzed later. The XKeystore program specifically collects and stores emails and nearly everything done on the Internet. A second program, PRISM, specifically targets non-American citizens by monitoring social media websites such as Facebook and also collects emails.

The massive data mining and storage is controversial for several reasons. First, most Americans feel they have an inalienable right to privacy protected by the Fourth Amendment and generally will not tolerate what they feel is government intrusion into their private lives. Nobody wants the government reading their emails or seeing who they are calling. However, after 9/11, many Americans were willing to sacrifice some privacy for the common good of stopping terrorists, but that support is slowing eroding. A second controversial aspect of the NSA surveillance programs is that American citizen's Internet metadata and phone records are being stored for an indefinite amount of time. Even though the NSA has FISC approved court orders and there is judicial and congressional oversight, the entire process is clouded in secrecy and few people know who is accessing the information, how often it is accessed and how it is being used. In other words, because the average American citizen and the media do not know exactly what the NSA is doing, there is a natural distrust. The NSA states that the archived phone records and metadata from the Internet help stop terrorist attacks and also aid in future investigations. Through the archived data, analysts are able to essentially go back in time, and review a target's contacts and establish a pattern of life that may lead to more hidden terrorists or uncover a terrorist cell, and hopefully stop them before they execute an attack. The NSA states that if they realize they are investigating an American citizen or person located in the United States, they will stop and seek a FISC court order to continue the investigation. The head of the NSA, General Keith Alexander, testified before Congress that the NSA does not read Americans' emails. "What you have is the date and time of the call, the calling number and the call — the duration of the call. And we also put in the origin of the metadata data. This does not include the content of the communications. This does not include your phone calls or mine, your emails, nor mine, your SMS messages. There is no content."[29] In response to a reporter's question

asking what the NSA does with all the metadata it stores, General Alexander responded, "Yeah, it sits there. And that's a great question because the court restricts what we can do with that data. We can only look at that data if we have a nexus to al-Qaida or other terrorist groups."[30]

Once explained properly, it is apparent that the established procedures put in place make sense and that the NSA is operating within the bounds of the Fourth Amendment. They legally collect phone records and Internet metadata. They do not listen to actual conversations or read actual emails unless the person is a foreigner located outside the United States. There are no laws curbing the targeting of foreign powers or persons so that is also legal. If, during their investigations, they need to investigate an American citizen or person located in the United States who has connections with a foreign power or persons, the NSA shows "probable cause" to FISC and acquire an approved court order and continue their investigation legally. Furthermore, the NSA is not the only organization that collects on Americans. Google, Yahoo, Facebook and other Internet companies also conduct massive data collection on people who use their websites. Actually, they created metadata first. Internet companies use metadata for social engineering and that gives the data unlimited commercial value. Through cookies and other data mining capabilities, the metadata can profile an individual and then offer web searches and advertising most appealing to that individual. For example, a Google web search will bring up different results for people based on their previous web searches. Lastly, these Internet companies will then sell that data to other companies to assist with their social engineering.[31] The point is, the NSA is not doing anything different than Internet companies by collecting massive amounts of metadata.

It seems then that the NSA's surveillance program is completely legal and adheres to the Fourth Amendment. However, critics still challenge the constitutionality in two ways. First,

despite the Supreme Court's ruling in *Smith vs. Maryland*, many feel that the creation of the Internet and its massive data collection capabilities requires a second look at protecting privacy. Whereas, public opinion and increased surveillance technology convinced the Court to overturn *Olmstead* and *Goldman* in *Katz vs United States*, the same could happen today with a public backlash towards the NSA and rapid growth of the Internet pervading every corner of our lives.

The second constitutional challenge is against the Foreign Intelligence Surveillance Court. In many ways, this is the most difficult challenge due to the classified nature of the Court. Critics argue that the FISC is unconstitutional because the approved court orders are kept secret and cannot be challenged in a criminal court of law. Criminal search warrants can be challenged if the evidence or procedures used to establish "probable cause" are questionable or done improperly. A FISC court order is not subject to due process because it is kept classified. The issue arises when FISA court orders are used in criminal trials. Never has a defendant been granted approval to view the FISC approved warrant and supporting documentation. Additionally, in a criminal court, defendants can question law enforcement officers to determine the validity of the search warrant and determine if any abuses occurred. Very rarely are intelligence agents or others involved in the surveillance process questioned about the FISC court order or evidence used to obtained it.[32] Instead, the process has created a perception that a FISC court order is above the law and impervious to challenges. Defendants are unable to determine if abuses or improper procedures have occurred that would invalidate the search warrant. Regrettably, people have to take the government's word that the court order was attained legally with no abuses.

Additionally, critics argue that FISC warrant requirements are less rigorous than their criminal surveillance counterparts when proving "probable cause." Due to lessened

requirements enacted by the Patriot Act and 2008 FISA Amendment Act, critics believe that a FISA court order can be obtained in cases where a criminal search warrant would be denied using the same justification.[33] In their article, Weaver and Pallitto, state that "representatives of the Justice Department admit that they view FISA as a preferred alternative to the Fourth Amendment warrants wherever such opportunities present themselves."[34] It is important to note that criminal activity cannot be the main purpose of obtaining a FISC court order. Collecting foreign intelligence has to be the "significant purpose." However, nothing stops a FISC court order from being used to prosecute individuals if illegal domestic criminal activity is uncovered during a foreign intelligence investigation.[35] Furthermore, critics also highlight the success rate of obtaining a FISC court order. Between 1979, when the court stood up, until 2012, only 11 of nearly 34,000 applications were rejected.[36] Critics argue that FISC is meaningless and exists only as a rubber stamp for unimpeded government surveillance.

Critics' final point against the NSA's surveillance programs counter the argument that the government is not collecting or storing anything different than what Internet companies already collect and store. Many Americans tolerate the collection of privacy metadata because it is protected under the 1974 Privacy Act and, more importantly, Internet companies do not generally have the motive or power to suppress political views. However, the United States government does possess the power to coerce their opponents. Information is powerful and governments around the world have previously used it to blackmail, suppress or purge their political rivals. Many believe the NSA's surveillance is the beginning of a slippery slope towards unimpeded government involvement in the privacy of its citizens similar to the worst case scenarios of Hitler's Gestapo, the East German Stasi or Stalin's repressive regime. One only needs to look at the Watergate example and President Nixon's attempt to spy on and

suppress his political rivals. What if the government was collecting disparaging information on a journalist and then used that information as leverage to stop the publishing of an article that may be unfavorable to the current administration? Another example would be the government using the archived metadata to determine the source of a journalist's article about leaked government secrets in order to identify and prosecute a whistleblower.

Supporters of the NSA's surveillance program argue that without it, the United States would be extremely vulnerable to another 9/11 type attack. Such an attack would have huge psychological and economic repercussions affecting not only the United States, but the world. They stress that the NSA is critical in detecting, tracking and stopping terrorists and insist that American citizens have nothing to fear unless they are involved in terrorist activities or supporting a foreign power to undermine the United States. They argue that the NSA is not interested in listening to every single phone call or reading every single email. First, there are too many and second, with limited manpower and funds, it is not efficient. Instead, the NSA uses classified programs, like PRISM and XKeystone, to archive the metadata so that it can be potentially used at a later date if needed during an official investigation backed by a FISC court order, and following the procedures set forth by the Fourth Amendment, FISA and the laws passed by Congress and signed by the President. While some civil liberties will be impinged upon, they argue that they are balanced with the interest of national security and not in conflict with the Constitution. Due to the classified nature of the surveillance techniques, sources and programs, Americans have to trust that the government is doing their job. Checks and balances were created by the Founding Fathers, and all three branches of government are ensuring that the civil liberties of American citizens and foreigners within the borders of the United States are protected. In 1978 Congress created FISA and passed multiple amendments to not only aid

intelligence agencies in the collection of information, but to also ensure the freedoms guaranteed in the Fourth Amendment were protected. The President worked with Congress to pass the laws, and then approved them. The Judicial branch has ruled on their constitutionality. Furthermore, the NSA has operated within the full scope of the law by acquiring search warrants from FISC when required and provided oversight reports to Congress when requested.

Edward Snowden has claimed that the United States has violated the Fourth Amendment by targeting phone records and emails of Americans. He stated that "the NSA specifically targets the communications of everyone. It ingests them by default. It collects them in its system and it filters them and it analyzes them and it measures them and it stores them for a period of time."[37] It has already been determined that the NSA does nothing illegal and operates within the boundaries of the law. Snowden argues that the storage of phone records and metadata is a violation of the Fourth Amendment, but is storing data and not looking at it unless a FISC court order is approved really a violation of privacy? Further justifying his actions Snowden also stated, "I, sitting at my desk, certainly had the authority to wiretap anyone, from you or your accountant, to a federal judge or even the President, if I had a personal email."[38] Of course Snowden had the job expertise and skills to accomplish those tasks, but should not do so without proper authorization in the form of a court order. However, Snowden does have a point when put in the context of violations by NSA employees. On August 15, 2013 the Washington Post reported that an internal audit showed that the NSA allegedly had violated its own rules thousands of times per year. An example used were NSA employees spying on love interests, known as LOV INT.[39] Inherent through their positions, NSA analysts are entrusted with huge responsibilities and a lot of power to detect and track terrorists and foreign operative. With that responsibility requires accountability. Thousands of violations each year give the perception that

there is either no oversight or no punishments for the violations. As with any large organization, violations will occur, and when they do happen, there has to be consequences.

SOLUTIONS

The NSA is in a precarious situation. They are not used to the public spotlight on their clandestine operations. While the leaks have severely damaged the United States' prestige and credibility throughout the world, the NSA would be irresponsible if they did not take the opportunity to change their organizational culture towards not only protecting the national security of the United States, but also protecting the cherished values enshrined in the Constitution. There are several solutions the NSA should attempt to institute. First, all NSA employees should receive mandatory training about the proper procedures of their positions and how breaking rules violates the Constitution and laws established by Congress. The training should be accomplished at least once a year and every time an employee commits a violation. The training should be administered by a lawyer and not a fellow NSA analyst or supervisor. With a lawyer, the training will not only be more comprehensive, but taken more seriously. Training given by a fellow NSA co-worker, as an additional duty, tends to be shorter and gives the impression of checking a training box rather than properly training NSA employees of the responsibilities and seriousness of their jobs. Also, lawyers could expertly answer any legality questions.

Second, an independent organization should be created to conduct periodic audits on the NSA, similar to the Inspector General for the USAF. Since policing themselves and lax Congressional oversight has resulted in thousands of violations each year, more robust oversight needs to be instituted. The independent organization should possess the same clearances and accesses to avoid security issues. Third, serious punishments have to be established and

enforced, including suspension or dismissal, if rules are intentionally or unintentionally broken. Currently, a reservist Marine may be forced to retire for sending classified information over an unclassified email. Such job discipline needs to be instilled to decrease violations and hold NSA employees accountable.

Fourth, the NSA needs to create a system that allows its employees to report violations, voice concerns or ask questions in a non-punitive anonymous environment. Such a system could potentially allow a future Edward Snowden to question the constitutionality of the surveillance programs without the risk of losing his job. If a lawyer could have explained how the NSA was adhering to the Constitution and laws, maybe he would not have felt impelled to defect and then release classified documents to highlight the issue. Additionally, such questions could be incorporated into the annual training to educate NSA employees and potentially head off any future doubt about the legality of their positions. Furthermore, it will be the employees that discover or highlight future violations of the Constitution and laws. When creating new procedures, mistakes sometimes happen. When violations are discovered, NSA leadership needs to address them appropriately and quickly. Lastly, the NSA's storage of phone records and metadata for indeterminate amounts of time concerns many Americans. Many Americans believe that the NSA will access them at will and ignore laws put in place. At least right now that is the perception with thousands of violations each year. The NSA Director stated that he did not care where the phone records and metadata were stored, as long they were stored where they could be accessed in the future.[40] Since telecommunication companies only have the ability to store records for a few months, an idea would be to provide federal money to increase their storage capability. That way the records are stored by a public company and not by the NSA.

This solution would be more palatable to those concerned about civil liberties. To access the data, the NSA would only need to provide a FISC court order.

President Obama's administration, along with the NSA Director and DNI, also need to accomplish a better job on the PR front. Without knowing exactly what is happening or how it is protecting the United States, Americans naturally think the worst and are paranoid that the government is watching their every move. President Obama, General Alexander and DNI Clapper need to explicitly explain how the Fourth Amendment is protected and how the NSA is staying within those bounds. They should also consider releasing redacted documents and information that will help improve transparency without comprising the intelligence methods and sources. Releasing terrorist attacks that the NSA surveillance programs helped thwart or information of how they obtained a FISC court order before investigating an American citizen would greatly assist in restoring faith and credibility in the surveillance programs. Lastly, the administration needs to take a more offensive approach in confronting future leaks by Edward Snowden. The NSA and President know what data was stolen, so the administration should be taking steps now to minimize future leaks and backlash. For example, the President should have talked to the French and German governments about the alleged spying on their citizens instead of waiting for Snowden to leak the disparaging information.

With its oversight power, Congress needs to either fix the perception, or consider laws to make FISC court orders and criminal search warrants equals in protecting against unreasonable searches and seizures. The perception is that FISC court orders are easily approved, but maybe FISC court order applications are not submitted unless the Justice Department and NSA are 100% positive it will be approved so they do not waste their time or the Court's time. That would explain why only 11 were rejected. If that is the case, then explain it to the press and

Americans. If that is not the case, then Congress has to ensure that FISC court orders meet the standards of protecting an individual's privacy while also meeting the "minimization" requirement set forth by FISA. If positive steps are not taken, public pressure and Supreme Court decisions could significantly limit what the NSA can do in the future. In 2012, Congress renewed the 2008 FISA Amendment Act for an additional five years, however, the votes in the Senate and House were far from unanimous. Additionally, after the Snowden incident in the summer of 2013, Congress was only 12 votes shy of drastically cutting funding for the NSA's surveillance programs.[41] As public support wanes, the NSA may find their job more difficult with more restrictive legislation, court decisions and reduced funding.

CONCLUSION

In conclusion, the NSA's surveillance programs are legal. The legal procedures created by FISA and its amendments, the Patriot Act, PAA and FAA, have thus far been upheld by the Judicial Branch as constitutional. However, if continued leaks by Edward Snowden continue to uncover alleged gross wrongdoings, public pressure could result in new legislation restricting the NSA abilities to collect intelligence within the United States. Additionally, law suits could be filed challenging the constitutionality of the surveillance programs, giving the Supreme Court an opportunity to reverse the *Smith* decision and declare all third party information such as phone records and Internet metadata as a "reasonable expectation of privacy." 9/11 happened 12 years ago and how quickly people forget the panic of that day. No longer does the government have the complete trust of the American people. While President Obama continues to stress that the NSA surveillance programs are for detecting and stopping terrorists, Americans cannot forget past abuses such as Watergate and President Bush's illegal TSP wiretapping program. The government needs to reestablish credibility by addressing negative perceptions, punishing

violations, releasing information verifying the effectiveness of the surveillance programs, and enact laws to not only continue to protect the Fourth Amendment, but punish any and all who purposely violate it.

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

[1] *Fourth Amendment, "Bill of Rights."*
[2] McKenzie, "What Were They Smoking?" 154.
[3] Davies, "The Supreme Court Giveth," 948-949.
[4] Ibid., 949.
[5] *Fourth Amendment, "Bill of Rights."*
[6] Davies, "The Supreme Court Giveth," 982.
[7] Ibid., 933.
[8] Ibid., 963.
[9] Clancy, "What is a Search," 17.
[10] Ibid., 17.
[11] Pesciotta, "I'm Not Dead Yet," 194.
[12] Clancy, "What is Search," 206.
[13] Ibid., 19.
[14] Davies, "The Supreme Court Giveth," 987.
[15] Ibid.," 987.
[16] *United States vs United States District Court*.
[17] Ibid.
[18] Johnson, "Surveillance and Privacy Under the Obama Administration," 421-422.
[19] Ibid., 421-422.
[20] Ibid., 423.
[21] Ibid., 423.
[22] CRS Report for Congress, 4.
[23] Ibid., 2.
[24] Ibid., 2.
[25] Johnson, "Surveillance and Privacy Under the Obama Administration," 428.
[26] Simmons, "Why 2007 is not Like 1984," 554.
[27] Ibid,. 555.
[28] Lanier, "The Meta Question," 20.
[29] Eddlem, "The NSA Domestic Surveillance Lie," 18.
[30] Ibid., 18.
[31] Lanier, "The Meta Question," 20-22.
[32] Pallitto and Weaver, "The Fourth Amendment and Foreign Intelligence Act," 5.
[33] Ibid., 7.
[34] Ibid., 7.
[35] Ibid., 7.
[36] McCutcheon, "Government Surveillance," 720.
[37] Eddlem, "The NSA Domestic Surveillance Lie," 18.
[38] Ibid., 18.
[39] Ibid., 19.
[40] McCutcheon, "Government Surveillance," 732.
[41] Ibid., 720.

Glossary

DNI - Director National Intelligence

FAA – FISA Amendment Act of 2008

FISA – Foreign Intelligence Act of 1978

FISC – Foreign Intelligence Surveillance Court

FISCR – Foreign Intelligence Surveillance Court Review

ISP – Internet Service Provider

NSA – National Surveillance Agency

PAA – Protect America Act of 2007

PATRIOT – Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

TSP – Terrorist Surveillance Program

Bibliography

Bazan, Elizabeth. "Foreign Intelligence Surveillance Act: A Sketch of Selected Issues." *Congressional Research Service Report for Congress* Order Code RL 34566 (7 Jul 2008): 1-14. http://web.ebscohost.com.aufric.idm.oclc.org/ehost/results?sid=b5c9168a-6405-4a0a-8189-ae6c95c99b62%40sessionmgr4002&vid=15&hid=4214&bquery=foreign+intelligence+surveillance+act%3a+a+sketch&bdata=JmRiPXRzaCZ0eXBlPTAmc2l0ZT1laG9zdC1saXZlJnNjb3BlPXNpdGU%3d (accessed 7 December, 2013).

Clancy, Thomas, K. "What is a "Search" Within the Meaning of the Fourth Amendment?" *Albany Law Review* 70 no. 1 (2006): 1-54. http://web.ebscohost.com.aufric.idm.oclc.org/ehost/results?sid=b5c9168a-6405-4a0a-8189ae6c95c99b62%40sessionmgr4002&vid=6&hid=4214&bquery=what+%22is%22+a+search+within&bdata=JmRiPXRzaCZ0eXBlPTAmc2l0ZT1laG9zdC1saXZlJnNjb3BlPXNpdGU%3d (accessed 7 December, 2013).

Davies, Thomas Y. "The Supreme Court Giveth and the Supreme Court Taketh Away: The Century of Fourth Amendment "Search and Seizure" Doctrine." *The Journal of Criminal Law and Criminology* 100 no. 93 (Summer 2010): 933-1041. http://web.ebscohost.com.aufric.idm.oclc.org/ehost/results?sid=b5c9168a-6405-4a0a-8189-ae6c95c99b62%40sessionmgr4002&vid=4&hid=4214&bquery=The+supreme+court+giveth&bdata=JmRiPXRzaCZ0eXBlPTAmc2l0ZT1laG9zdC1saXZlJnNjb3BlPXNpdGU%3d (accessed 7 December, 2013).

Eddlem, Thomas. "The NSA Surveillance Lie." *New American*, 7 October 2013, 17-19.

Fourth Amendment, "Bill of Rights." Washington DC, 1791

Johnson, Elizabeth. "Surveillance and Privacy Under the Obama Administration: Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 and the Attorney General's Guidelines for Domestic FBI Operations." *Journal of Law and Policy for the Information Society* 6 no. 1 (2009): 419-446. http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Johnson.pdf (accessed 7 December, 2013).

Lanier, Jaron. "The Meta Question." *Nation* 297 no. 1/2 (8 July, 2013): 20-23. http://web.ebscohost.com.aufric.idm.oclc.org/ehost/detail?vid=21&sid=b5c9168a-6405-4a0a-8189-ae6c95c99b62%40sessionmgr4002&hid=4214&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#db=tsh&AN=88786295 (accessed 7 December, 2013).

McCutcheon, Chuck. "Government Surveillance." *CQ Researcher* 23, no. 30 (30 August 2013): 717-740.

McKenzie, Daniel. "What Were They Smoking?: The Supreme Court's Latest Step in a Long, Strange Trip Through the Fourth Amendment." *The Journal of Criminal Law and Criminology* 93, no. 1 (Fall 2002): 153-194. http://web.ebscohost.com.aufric.idm.oclc.org/ehost/detail?vid=3&sid=b5c9168a-6405-4a0a-8189-ae6c95c99b62%40sessionmgr4002&hid=4214&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#db=tsh&AN

=10026607 (accessed 7 December, 2013).

Pallitto, Robert M., and William G. Weaver. "The Foreign Intelligence Surveillance Act and the Fourth Amendment." *All Academic Research Inc*., 2003, 1-66. http://citation.allacademic.com/meta/p_mla_apa_research_citation/0/6/2/0/6/pages62068/p62068-1.php (accessed 7 December, 2013).

Pesciotta, Daniel T. "I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century." *Case Western Reserve Law Review* 63, no. 1 (Fall 2012): 187-255. http://web.ebscohost.com.aufric.idm.oclc.org/ehost/results?sid=b5c9168a-6405-4a0a-8189ae6c95c99b62%40sessionmgr4002&vid=7&hid=4214&bquery=katz%2c+jones+AND+the+fourth+amendment&bdata=JmRiPXRzaCZ0eXBlPTAmc2l0ZT1laG9zdC1saXZlJnNjb3BlPXNpdGU%3d (accessed 7 December, 2013).

Simmons, Ric. "Why 2007 is not Like 2008: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence." *The Journal of Criminal Law and Criminology* 97, no. 2 (Winter 2007): 531-568. http://web.ebscohost.com.aufric.idm.oclc.org/ehost/detail?vid=19&sid=b5c9168a-6405-4a0a-8189-ae6c95c99b62%40sessionmgr4002&hid=4214&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#db=tsh&AN=25643758 (accessed 7 December, 2013).

United States vs United States District Court. In Cornell Law Synopsis Website. http://www.law.cornell.edu/supct/html/historics/USSC_CR_0407_0297_ZS.html (accessed 7 December, 2013).